JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 26, 2001

Application Number: 2001-087799

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

October 26, 2001

Commissioner,
Japan Patent Office

Kozo Oikawa

Number of Certification: 2001-3093625

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-261217
(43)Date of publication of application : 03.10.1997

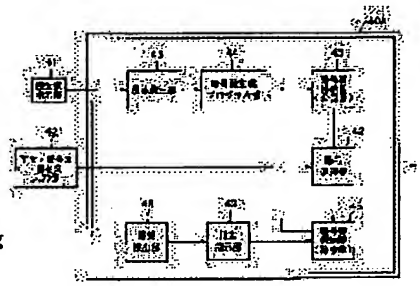
(51)Int.Cl. H04L 9/10
G09C 1/00
G09C 1/00
H04L 9/30
H04L 9/32

(21)Application number : 08-072949
(22)Date of filing : 27.03.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : ISHII SHINJI

(54) COMMUNICATION EQUIPMENT AND ITS METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To generate the key of an open key password without requiring a specified device by providing a means for generating an open key required to inspect a secret key necessary for a signature and the signature inside damper mechanism.
SOLUTION: In a device where ciphered digital data is received, the reception is proved by utilizing the digital signature and ciphered digital data is decoded and processed, a random number generating part 43 and a passward key generating program part 44 generate the key of the open key password in accordance with an instruction from a key generation indicating part 41. An open key storing part 45 storing a decoding key for decoding ciphered digital data, a secret key storing part 46 storing a decoding key for decoding ciphered digital data and a password processing part 47 decoding ciphered digital data are arranged inside damper mechanism from which data is not taken out so as to prevent the illegal copying of digital data. The means for generating the necessary open key in order to insect the secret key requiured for the signature and the signature is provided inside damper mechanism.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－261217

(43)公開日　平成９年(1997)10月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ａ
Ｇ０９Ｃ	1/00	６２０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６２０Ｂ
		６４０	7259－5Ｊ			６４０Ｂ
Ｈ０４Ｌ	9/30			Ｈ０４Ｌ	9/00	６６３Ｂ
	9/32					６７５Ｂ

審査請求　未請求　請求項の数８　ＯＬ　（全７頁）

(21)出願番号　特願平8－72949

(22)出願日　平成８年(1996)３月27日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　石井　晋司
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内

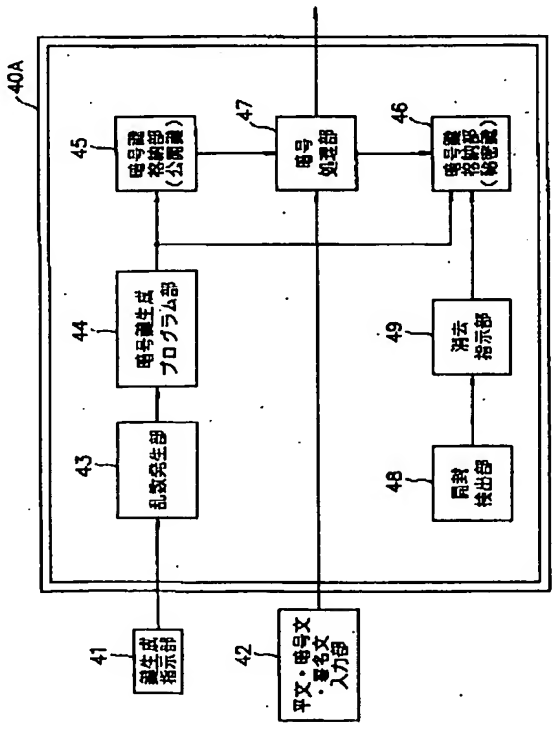
(74)代理人　弁理士　吉田　精孝

(54)【発明の名称】　通信装置及びその方法

(57)【要約】

【課題】　特別な装置を必要とすることなく公開鍵暗号の鍵を生成し得る通信装置及びその方法を提供すること。

【解決手段】　鍵生成指示部４１からの指示に従って公開鍵暗号の鍵を生成する乱数発生部４３及び暗号鍵生成プログラム部４４と、該生成した鍵を格納する暗号鍵格納部４５，４６と、平文・暗号文・署名文入力部４２から入力される平文または暗号文もしくは署名文を前記鍵を用いて暗号化しまたは復号しもしくは署名する暗号処理部４７とを、開封検出部４８により開封を検出すると消去指示部４９によって暗号鍵格納部４６に格納した秘密鍵を消去する個人携帯デバイス４０の被い４０Ａ内に設けておくことにより、該デバイス４０がない限り情報を利用できないようにして不正コピーを防止する。



【特許請求の範囲】

【請求項１】　暗号化されたディジタルデータを受信し、該受信をディジタル署名を利用して証明し、前記暗号化されたディジタルデータを復号して何人にも知られないように処理する装置であって、署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、暗号化されたディジタルデータを復号する復号鍵を記憶する復号鍵記憶手段と、暗号化されたディジタルデータを復号する暗号化データ復号手段とを、データの取り出しが不能なタンパ機構内に配置することによりディジタルデータの不正コピーを防止した通信装置において、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段をタンパ機構内に設けたことを特徴とする通信装置。

【請求項２】　ディジタルデータとして符号化された情報もしくは実行プログラムを用いたことを特徴とする請求項１記載の通信装置。

【請求項３】　タンパ機構に属する手段のうち少なくとも秘密鍵記憶手段と復号鍵記憶手段と鍵生成手段とを、タンパ機能を有しかつ携帯可能で本体に対しデータのやりとりが可能な筐体内に配置したことを特徴とする請求項１または２記載の通信装置。

【請求項４】　情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信したディジタルに符号化された情報を受信者が確かに受信したことを証明することと、符号化されたディジタル情報を復号した状態で利用することはできるが、そのディジタル情報をコピーすることはできないようにするために、

発信側の装置は、

符号化されたディジタル情報を暗号化する送信側暗号化手段と、

暗号化したディジタル情報を受信側に送る暗号化データ送信手段とを具備し、

受信側の装置は、

暗号化データを受信する暗号化データ受信手段と、

暗号化されたディジタルデータを復号する暗号化データ復号手段と、

符号化されたディジタルデータを復号する符号化データ復号手段と、

暗号化データ復号手段と符号化データ復号手段とを連結する連結手段と、

連結手段のディジタルデータを何人にも知られないようにするための再生用タンパ機構と、

暗号化データを復号する復号鍵を保持する復号鍵記憶手段と、

暗号化されたデータを受信したことをディジタル署名を利用して証明する署名手段と、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段と、

署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、

署名の検証に必要な公開鍵を公開する公開鍵出力手段と、

復号鍵記憶手段、鍵生成手段及び秘密鍵記憶手段の入出力結果を何人にも知られないようにするための鍵用タンパ機構とを具備したことを特徴とする通信装置。

【請求項５】　情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信した実行プログラムを受信者が確かに受信したことを証明することと、受信した実行プログラムを実行することはできるが、プログラムをコピーすることはできないようにするために、

発信側の装置は、

実行プログラムを暗号化する送信側暗号化手段と、

暗号化した実行プログラムを受信側に送る暗号化データ送信手段とを具備し、

受信側の装置は、

暗号化データを受信する暗号化データ受信手段と、

暗号化された実行プログラムを復号する暗号化実行プログラム復号手段と、

実行プログラムを実行するプログラム実行手段と、

暗号化実行プログラム復号手段とプログラム実行手段とを連結する連結手段と、

連結手段の復号後のディジタルデータを何人にも知られないようにするためのプログラム実行用タンパ機構と、

暗号化データを復号する復号鍵を保持する復号鍵記憶手段と、

暗号化されたデータを受信したことをディジタル署名を利用して証明する署名手段と、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段と、

署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、

署名の検証に必要な公開鍵を公開する公開鍵出力手段と、

復号鍵記憶手段、鍵生成手段及び秘密鍵記憶手段の入出力結果を何人にも知られないようにするための鍵用タンパ機構とを具備したことを特徴とする通信装置。

【請求項６】　鍵用タンパ機構に属する手段を備えた携帯可能な筐体と、鍵用タンパ機構に属する手段を除いた受信側の装置とを具備し、前記筐体と受信側の装置とのそれぞれにデータのやりとりを行うインタフェース手段を設けたことを特徴とする請求項４または５記載の通信装置。

【請求項７】　情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信したディジタルに符号化された情報を受信者が確かに受信したことを証明することと、符号化されたディジタル情報を復号した状態で利用することはできるが、そのディジタル情報をコピーすることはできないようにするために、

送信側では、

符号化されたディジタル情報を暗号化し、

該暗号化したディジタル情報を受信側に送り、
受信側では、
ネットワークを介して暗号化データを受信し、
暗号化の復号と符号化の復号を行う部分のディジタルデータを何人にも知られないようにし、
暗号化データを復号する鍵を保持し、
暗号化されたデータを受信したことをディジタル署名を利用して証明し、
ディジタル署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成し、
署名に必要な秘密鍵を記憶し、
署名の検証に必要な公開鍵を公開し、
暗号化されたディジタルデータを復号し、
符号化されたディジタルデータを復号し、
ディジタルデータの復号鍵、署名用の鍵生成及び署名用の秘密鍵の入出力結果を何人にも知られないようにすることを特徴とする通信方法。
【請求項８】　情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信した実行プログラムを受信者が確かに受信したことを証明することと、発信側の手順として実行プログラムを復号した状態で利用することはできるが、その実行プログラムをコピーすることはできないようにするために、
送信側では、
実行プログラムを暗号化し、
暗号化した実行プログラムを受信側に送り、
受信側では、
ネットワークを介して暗号化データを受信し、
暗号化の復号と実行プログラムを実行する部分のディジタルデータを何人にも知られないようにし、
暗号化データを復号する鍵を保持し、
暗号化されたデータを受信したことをディジタル署名を利用して証明し、
ディジタル署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成し、
署名に必要な秘密鍵を記憶し、
署名の検証に必要な公開鍵を公開し、
暗号化された実行プログラムを復号し、
必要ならば実行プログラムを実行し、
ディジタルデータの復号鍵、署名用の鍵生成及び署名用の秘密鍵の入出力結果を何人にも知られるないようにすることを特徴とする通信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、特別な装置を必要とすることなく公開鍵暗号の鍵を生成し得る通信装置及びその方法に関するものである。
【０００２】
【従来の技術】音声・映像情報や実行プログラムのような著作権を有するディジタルデータを、ネットワークを利用して販売しようとする場合、利用者認証及び配送確認とともに不正コピーの防止が問題となる。
【０００３】利用者認証を解決する方法としては、ディジタル暗号アルゴリズムの公開鍵暗号を利用する方法がある。以下、公開鍵暗号について簡単にふれておく。
【０００４】ディジタル暗号アルゴリズムには、共通鍵暗号アルゴリズム（秘密鍵暗号アルゴリズム）と公開鍵暗号アルゴリズムとがある。
【０００５】共通鍵暗号アルゴリズムは、高速演算が可能であるが、暗号化鍵と復号鍵に同じ共通鍵を使用することから、通信する両者のみがその共通鍵を秘密に保持する必要がある。一方、公開鍵暗号アルゴリズムは、共通鍵暗号アルゴリズムに比べて計算量が多く、高速処理には不向きであるが、暗号化鍵と復号鍵に異なる鍵を使用するため、暗号化鍵を公開しておくことにより、共通鍵暗号アルゴリズムの共通鍵のように鍵を秘密に配送する必要がなくなる。
【０００６】ところが、公開鍵暗号アルゴリズムでは、暗号化鍵を公開していることから誰もが暗号文を作成することができる。このため、暗号化されて送られてきた通信文等を、誰が暗号化して送ってきたかを証明することも必要になる。そこで、考えられるようになったのが署名を利用した相手認証である。
【０００７】相手認証機能を備えた公開鍵暗号アルゴリズムの代表例として、ＲＳＡ暗号がある。これは暗号通信に関して、暗号化する時には暗号化鍵を利用し、復号する時には復号鍵を利用し、また、署名を生成する時は復号鍵を利用し、その署名を検証する時は暗号化鍵を利用するものである。
【０００８】一方、配送すべきディジタルデータを暗号化するには、公開鍵暗号ではなく共通鍵暗号が使われることがほとんどである。その最大の理由は、非常に大きなディジタルデータの暗号処理には、公開鍵暗号に比べて極めて高速な共通鍵暗号の方が適しているからである。
【０００９】
【発明が解決しようとする課題】しかし、共通鍵暗号アルゴリズムでは、通信する両者が共通の秘密鍵を所有していなければならない。そこで、共通鍵暗号に使う共通の秘密鍵を公開鍵暗号を利用して相手を認証し、配送することが一般的である。しかし、それだけでは利用者のコピーは防ぐことはできない。そこで、利用者認証に用いる秘密鍵を、タンパ機構（装置）を用いることにより誰にも知られることのないようにして、個人携帯デバイスを作成できることを特徴とした発明（特願平７－１５５０３０号、特願平７－１５９４１４号、特願平７－２０４６４２号）を提案した。しかし、これらの発明では、個人携帯デバイスにユーザの秘密鍵を埋め込むためのタンパ装置が必要になるという問題があった。
【００１０】本発明の目的は、特別な装置を必要とする

ことなく公開鍵暗号の鍵を生成し得る通信装置及びその方法を提供することにある。

【００１１】

【課題を解決するための手段】本発明では、前記課題を解決するため、暗号化されたディジタルデータを受信し、該受信をディジタル署名を利用して証明し、前記暗号化されたディジタルデータを復号して何人にも知られないように処理する装置であって、署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、暗号化されたディジタルデータを復号する復号鍵を記憶する復号鍵記憶手段と、暗号化されたディジタルデータを復号する暗号化データ復号手段とを、データの取り出しが不能なタンパ機構内に配置することによりディジタルデータの不正コピーを防止した通信装置において、署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段をタンパ機構内に設けた。

【００１２】ネットワークを利用したディジタル情報販売システムでは、本人を含めて誰もが知らない本人の秘密鍵と、本人しか所有していない秘密鍵を特別な専用装置なしに生成することができることから、・本人の確認のために相手認証機能を行える、・ディジタル著作権情報を購入した本人でさえ、不正コピーをすることができないシステムを提供することができる。

【００１３】

【発明の実施の形態】以下、図面に従って本発明の実施の形態を説明するが、ここでは公開鍵暗号アルゴリズムの中で暗号機能と認証機能を合わせ持ち、最も広く利用されているＲＳＡ暗号を用いて説明する。なお、ＲＳＡ暗号の詳細については、池野、小山共著 社団法人電子情報通信学会編「現代暗号理論」の「第６章 ＲＳＡ公開鍵暗号」に詳述されている。

【００１４】（第１の形態）図１は本発明を利用してサービスを行うシステム全体の基本的な構成を示すもので、図中、１０はコンテンツサーバ、２０はネットワーク、３０は個人用端末、４０は個人携帯デバイスである。

【００１５】コンテンツサーバ１０はサービスを提供する。サービスを利用する者が、個人用端末３０に個人携帯デバイス４０を差し込み、該個人用端末３０を操作することにより、コンテンツサーバ１０からネットワーク２０を介して個人用端末３０にコンテンツを配布させる。

【００１６】図２は個人携帯デバイス４０の詳細を示すもので、図中、４１は鍵生成指示部、４２は平文・暗号文・署名文入力部、４３は乱数発生部、４４は暗号鍵生成プログラム部、４５，４６は暗号鍵格納部、４７は暗号処理部、４８は開封検出部、４９は消去指示部である。

【００１７】前記構成中、鍵生成指示部４１及び平文・暗号文・署名文入力部４２を除く部分は、いかなる者もその内部に触れることができない被い（タンパ機構）４０Ａの中である。例え、この個人携帯デバイス４０の所有者であっても被い４０Ａを無理に開けて、内部に保存されているＲＳＡ暗号の秘密鍵を読み出そうとすると、開封検出部４８が開封を検出し、消去指示部４９により内部の秘密情報を電気的に消去する。また、違う鍵に書き換えたりすることもできないように、開封すると個人携帯デバイス４０の内部で使用している半導体チップの端子や基盤の配線も壊れるように製造してある。

【００１８】個人携帯デバイス４０は、２つの入力系と１つの出力系を備えている。入力系のうちの１つはＲＳＡ暗号の鍵生成指示部４１である。これは、ユーザがこの個人携帯デバイス４０を利用してサービスを受けようとする前に、今後、使用するＲＳＡ暗号の公開鍵と秘密鍵を生成する指示である。鍵生成指示部４１によって指示される具体的な例は、乱数発生部４３で使用する乱数のシード（種）である。

【００１９】ここで使用するシードはほぼ２度と同じシードを発生することのない方法がふさわしい。例えば、キーボード入力の入力文字とその入力時間間隔を利用するのが実用的である。入力されたシードは、乱数発生部４３で乱数となり、暗号鍵生成プログラム部４４に与えられる。暗号鍵生成プログラム部４４はＲＳＡ暗号の鍵を生成する。暗号鍵生成プログラム部４４で生成されたＲＳＡ暗号の鍵のうち、公開鍵は公開する必要があるので、個人携帯デバイス４０の外部から読み出しが可能な公開鍵格納部４５に格納される。一方、秘密鍵の方は読み出すことができないように秘密鍵格納部４６に格納される。

【００２０】以上で個人携帯デバイス４０の内部で使用する鍵の準備は終了である。

【００２１】サービスを受ける場合、平文の暗号化／暗号文の復号、署名／検証が必要になったときにパラメータがもう１つの入力系、つまり平文・暗号文・署名文入力部４２に入力される。入力された平文の暗号化及び署名文の検証には、相手の公開する公開鍵を使用する。暗号文の検証には、秘密鍵格納部４６の秘密鍵を利用して、暗号処理部４７にて演算し出力される。

【００２２】このようにして生成したＲＳＡ暗号の秘密鍵は、個人携帯デバイス４０を所有するものだけが使用することができることを誰にでも納得させることができ、かつ秘密鍵の値そのものは個人携帯デバイス４０を所有するものも含めて誰も知ることができないことを誰もが納得することができる。

【００２３】言い換えると本発明の課題であった、・本人の確認のために相手認証機能を行える、・ディジタル著作権情報を購入した本人でさえ、不正コピーをすることができないシステムを提供することができ、しかも、個人携帯デバイス４０で使用する秘密鍵を特別な装置なしに実現することができる。

【００２４】個人携帯デバイス４０の実際の例としては、規格化されているＩＣカード、ＰＣカード（ＰＣＭＣＩＡ）を用いて容易に実現できる。

【００２５】また、受信側で実際に復号したコンテンツを利用する方法としては、特願平６－２９８７０２号、特願平６－２９９９４０号で提案したものがある。

【００２６】なお、鍵生成指示部４１及び平文・暗号文・署名文入力部４２は本デバイス４０を差し込む個人用端末３０側に設けても良く、また、個人用端末３０と個人携帯デバイス４０とを一体化することもできる。

【００２７】図３は個人情報デバイスにおける鍵生成手順を示すフローチャートである。

【００２８】最初に、個人携帯デバイス４０の所有者が、鍵生成開始を指示する（ｓ１）。この指示により、個人携帯デバイス４０は乱数用シードを作成する（ｓ２）。その後、これを利用して乱数を生成し（ｓ３）、鍵生成プログラムを起動し（ｓ４）、鍵を生成する。生成した鍵のうち、公開鍵は通信相手に配布する必要があるので、個人携帯デバイス４０から出力する（ｓ５）。出力された公開鍵を個人携帯デバイス４０の所有者が受け取り（ｓ６）、必要ならば、証明書発行機関などに公開鍵を登録し、承認された後、その公開鍵を通信相手に配布する。

【００２９】一方、個人携帯デバイス４０は、秘密鍵を個人携帯デバイス４０の秘密鍵読み出し不可領域に格納し（ｓ７）、鍵生成を終了する。

【００３０】図４は個人情報デバイスにおける鍵消去手順を示すフローチャートである。

【００３１】個人携帯デバイス４０の所有者を含めた何者かが、個人携帯デバイス４０の内部の秘密情報を取り出すために、細工をしようとする場合を想定する。最初は、個人携帯デバイス４０と個人用端末３０とのインタフェースから何らかの秘密情報が取り出せないかどうか試みると考えられる。しかしながら、当然公開可能な情報以外は出力されないので、秘密情報を得ることはできない。そこで、ここであきらめない場合、個人携帯デバイス４０の中を開封し、秘密情報を取り出そうと試みると考えられる。

【００３２】もし、少しでもデバイスのケースをこじ開けようとする（ｓｐ１）と、デバイス開封が検出され（ｓｐ２）、秘密鍵消去プログラムが起動されて（ｓｐ３）、秘密鍵が消去される（ｓｐ４）。

【００３３】また、個人携帯デバイス４０を無理にこじ開ける（ｓｐ５）と、搭載された主なチップが破壊され（ｓｐ６）、情報の取り出しは不可能となる。

【００３４】このように、たとえ個人携帯デバイス４０を開封し、秘密情報を得ようとしても不可能である。

【００３５】

【発明の効果】以上説明したように、本発明によれば、個人携帯デバイスを用いて、誰もが知り得ない公開鍵暗号の秘密鍵をユーザのみが使用できる証明をすることができる個人用の秘密鍵を特別な専用装置を用いることなく生成することができる。

【００３６】この個人携帯デバイスを使用することにより、特別なネットワーク上でディジタル情報を商品として取り扱う場合に、支払い意志を表明したものはユーザが唯一であることが証明でき、かつユーザがディジタル情報を情報提供者に無断でコピーできないことが証明できるようになる効果がある。

【図面の簡単な説明】

【図１】本発明を利用してサービスを提供するシステム全体の構成図

【図２】個人携帯デバイスの詳細を示す構成図

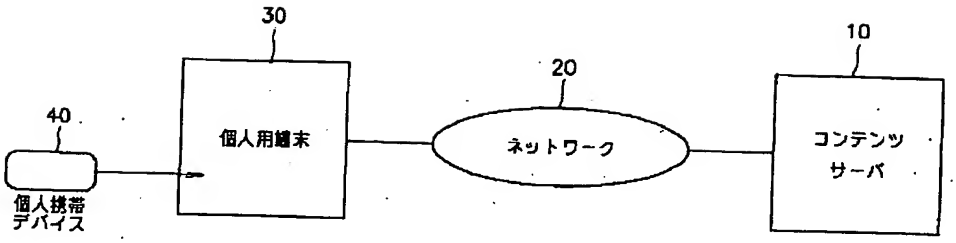
【図３】個人携帯デバイスにおける鍵生成手順を示すフローチャート

【図４】個人携帯デバイスにおける鍵消去手順を示すフローチャート

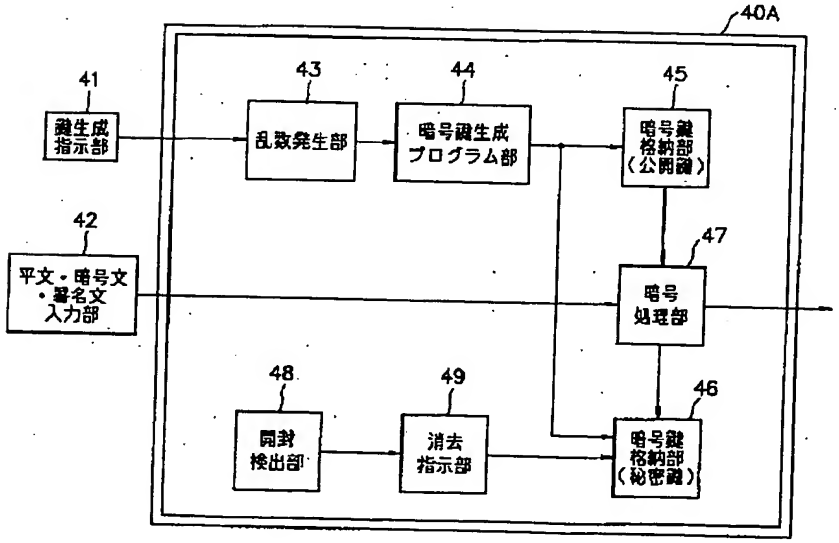
【符号の説明】

１０…コンテンツサーバ、２０…ネットワーク、３０…個人用端末、４０…個人携帯デバイス、４１…鍵生成指示部、４２…平文・暗号文・署名文入力部、４３…乱数発生部、４４…暗号鍵生成プログラム部、４５，４６…暗号鍵格納部、４７…暗号処理部、４８…開封検出部、４９…消去指示部、４０Ａ…被い。

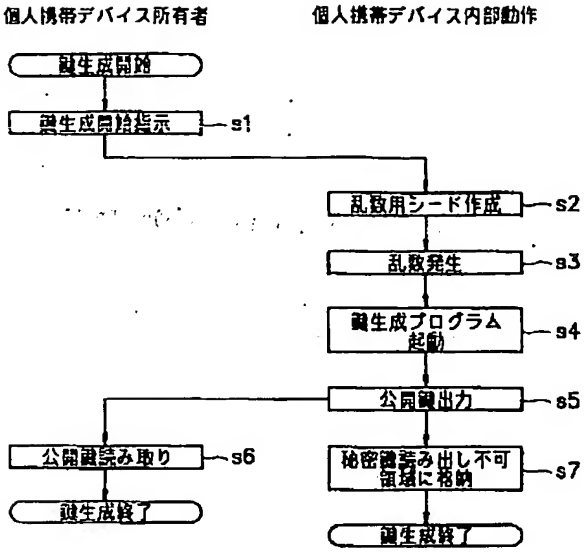
【図１】


30
10
20
40
個人用端末
ネットワーク
コンテンツ
サーバ
個人携帯
デバイス

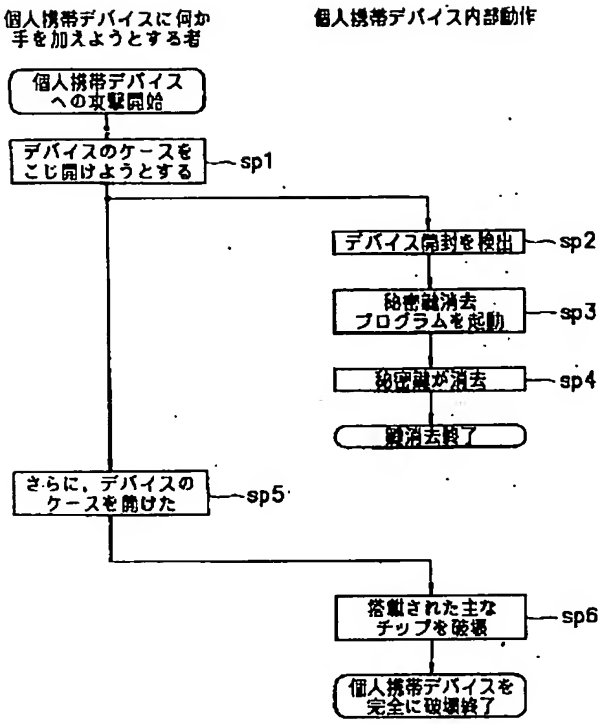
【図２】


40A
41
43
44
45
鍵生成
指示部
乱数発生部
暗号鍵生成
プログラム部
暗号鍵
格納部
（公開鍵）
42
47
平文・暗号文
・署名文
入力部
暗号
処理部
48
49
46
開封
検出部
消去
指示部
暗号鍵
格納部
（秘密鍵）

【図３】


個人携帯デバイス所有者
個人携帯デバイス内部動作
鍵生成開始
鍵生成開始指示
s1
乱数用シード作成
s2
乱数発生
s3
鍵生成プログラム起動
s4
公開鍵出力
s5
公開鍵読み取り
s6
秘密鍵を読み出し不可領域に格納
s7
鍵生成終了
鍵生成終了

【図４】


個人携帯デバイスに何か手を加えようとする者
個人携帯デバイス内部動作
個人携帯デバイスへの攻撃開始
デバイスのケースをこじ開けようとする
sp1
デバイス開封を検出
sp2
秘密鍵消去プログラムを起動
sp3
秘密鍵が消去
sp4
鍵消去終了
さらに，デバイスのケースを開けた
sp5
搭載された主なチップを破壊
sp6
個人携帯デバイスを完全に破壊終了